(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 722 596**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **94 08770**

(51) Int Cl⁶ : G 07 C 9/00, G 06 F 12/14

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 13.07.94.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 19.01.96 Bulletin 96/03.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *FRANCE TELECOM ETABLISSEMENT PUBLIC* — FR et *LA POSTE* — FR.

(72) **Inventeur(s) :** GIRAULT MARC, REITTER RENAUD et REVILLET MARIE JOSEPHE.

(73) **Titulaire(s) :**

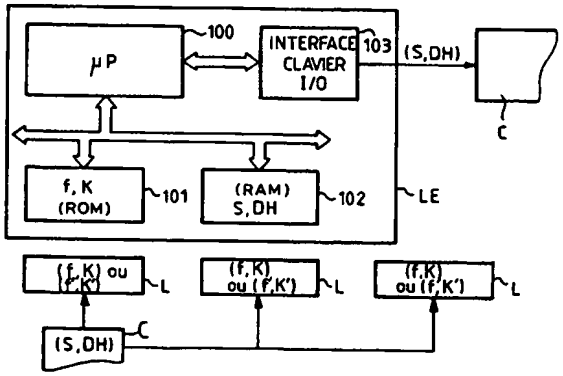
(74) **Mandataire :** CABINET BALLOT SCHMIT.

(54) SYSTEME DE CONTROLE D'ACCES LIMITES A DES PLACES HORAIRES AUTORISEES ET RENOUVABLES AU MOYEN D'UN SUPPORT DE MEMORISATION PORTABLE.

(57) L'invention concerne un système de contrôle d'accès limités à des plages horaires autorisées et renouvelables au moyen d'un support de mémorisation portable.

Le système comporte pour cela un organe (LE) produisant des clés électroniques composées d'une donnée relative à une plage horaire et de la signature de cette donnée. Ces clés sont chargées dans des supports tels que des cartes à mémoire (c). Des serrures électroniques (L) aptes à vérifier les signatures sont implantées à différents emplacements (physiques ou logiques) dont on veut protéger l'accès.

Application au contrôle d'accès de bâtiments ou de systèmes informatiques.



FR 2 722 596 - A1

SYSTEME DE CONTROLE D'ACCES LIMITES A DES PLAGES HORAIRES AUTORISEES ET RENOUVELABLES AU MOYEN D'UN SUPPORT DE MEMORISATION PORTABLE

L'invention concerne un système de contrôle d'accès limités à des plages horaires autorisées et renouvelables au moyen d'un support de mémorisation .

L'invention s'applique tout particulièrement au domaine du contrôle d'accès à des bâtiment, à des systèmes informatiques ou à toutes sortes d'objets dont l'ouverture ou l'utilisation doit être contrôlée.

La manière la plus connue de verrouiller un accès qu'il s'agisse d'un bâtiment ou de tout autre objet consiste à placer une serrure mécanique et à délivrer une clé aux personnes ayant une autorisation d'accès. Bien entendu, l'inconvénient de cette méthode réside dans le fait que les clés mécaniques sont parfaitement duplicables. Une telle clé peut être également volée et utilisée par le voleur, la seule solution possible étant alors de changer le barillet de la serrure.

Une deuxième méthode, mais électronique celle-ci consiste à prévoir une serrure avec mot de passe. Seuls les utilisateurs connaissant le mot de passe sont habilités à accéder au bâtiment protégé.

Malheureusement, cette solution n'est pas infaillible. En effet, lorsqu'un utilisateur entre son mot de passe en le tapant sur un clavier, il est tout à fait possible à ce moment-là de concevoir une électronique apte à lire ce mot de passe au passage et, par conséquent, à permettre à une personne mal intentionnée de le réutiliser.

On connaît également une procédure d'authentification dénommée Kerberos qui permet de protéger l'accès à un réseau informatique ouvert. On trouvera une description de cette procédure dans la publication du 30 mars 1988 du MIT, intitulée "An Authentification Service for Open Network Systems".

Cette procédure permet d'identifier un "client", c'est à dire un utilisateur et de lui permettre un accès à un serveur (à un service, une application, un programme) en lui délivrant pour cela un ticket électronique et plus précisément une information cryptée au moyen d'une clé. Ce ticket est établi par le serveur au "client". D'autre part, le ticket n'est pas suffisant pour obtenir l'autorisation d'accès, une deuxième information cryptée est également utilisée dans la procédure en combinaison avec l'utilisation du ticket.

Une telle procédure est lourde et demande des moyens de calcul relativement puissant, ce qui n'est pas une contrainte dans l'application qui est donnée, mais qui peut le devenir pour toute autre application, applications pour lesquelles la place mémoire et les moyens de calculs ne sont pas aussi importants que ceux d'un serveur.

D'autre part, la deuxième information cryptée est établie pour un accès entre un client et un serveur et ne peut être utilisée qu'une fois pour cette liaison.

La présente invention a pour but de remédier à ces inconvénients.

D'autre part, selon l'invention, il n'est plus nécessaire d'avoir à constituer une liste noire de moyens d'accès perdus ou volés ou dupliqués et d'avoir à gérer de telles listes car, comme on le verra dans la suite de la description, un support volé ou perdu ne

pourra donner droit à un accès en dehors de la plage horaire autorisée si celle-ci n'est pas renouvelée. L'inscription de ce support sur une liste noire sera d'autant plus inutile que la durée d'autorisation d'accès sera courte.

Conformément à l'invention, le contrôle d'accès est réalisé non pas par des moyens mécaniques mais par des moyens logiques faisant intervenir une signature électronique de données relatives à une période prédéterminée d'autorisation d'accès limitant la validité d'utilisation du support dans lequel elle est mémorisée. En effet selon l'invention, la signature est mémorisée dans le support de mémorisation portable ainsi que selon l'algorithme utilisé, la donnée afin de permettre des accès à tous les équipements comportant le système de protection conforme à l'invention.

La présente invention a plus particulièrement pour objet : un système de contrôle d'accès au moyen d'un support de mémorisation portable, principalement caractérisé en ce qu'il comporte :

1°) des moyens aptes à délivrer des clés électroniques formées au moins de données DH et de la signature d'au moins ces données, ces moyens étant aptes à élaborer les signatures électroniques S des données DH relatives à une période prédéterminée d'autorisation d'accès et de charger les signatures S dans les supports de mémorisation respectifs, une signature devant être recalculée pour établir le renouvellement des périodes d'autorisation d'accès.

2°) des moyens assurant une fonction de serrure électronique aptes à délivrer un signal d'autorisation d'accès dans le cas où le support de mémorisation comporte en mémoire la donnée et

la signature requise, ces moyens étant aptes à vérifier que la donnée est bien la donnée attendue et que la signature est la signature de cette donnée.

Le terme signature électronique doit être entendu ici au sens large. Il peut s'agir d'une signature électronique obtenue à l'aide de tout mécanisme cryptographique connu, à savoir des mécanismes de chiffrement ou d'authentification.

De préférence la donnée DH relative à la période prédéterminée de validité comporte une information de date d'utilisation et une plage horaire d'utilisation.

Selon un mode de réalisation, la signature est obtenue au moyen d'un algorithme de production à clé secrète.

Selon un autre mode de réalisation, la signature peut être obtenue au moyen d'un algorithme de production à clé publique.

Selon l'invention, la signature sera obtenue préférentiellement avec un algorithme à clé publique dans le cas d'application de type usage public, c'est à dire dans le cas où la vérification de la signature va se faire à partir de moyens placés dans un environnement public.

Selon un autre mode de réalisation, la clé utilisée pour élaborer les signatures est la même pour toutes les signatures chargées dans les supports et renouvelées.

Selon une autre caractéristique de l'invention, on associe à cette clé K une donnée Z distincte selon les zones géographiques ou logiques d'utilisation afin de pouvoir distinguer ces zones d'utilisation.

Selon un autre mode de réalisation, on utilise des clés différentes pour élaborer les signatures chargées

périodiquement, une clé étant choisie par zone géographique ou logique déterminée.

Selon une autre caractéristique de l'invention, on pourra utiliser une clé diversifiée Kc produite à partir d'une fonction de diversification de type connu.

Selon une autre caractéristique de l'invention, on divise la plage horaire de validité déterminé en un nombre donné de plages horaire consécutives et, on élabore une signature Si pour chacune de ces plages.

L'invention sera mieux comprise à l'aide de la description qui est donnée à titre indicatif et non limitatif et en regard des dessins sur lesquels :

- la figure 1 représente le schéma de principe d'un système objet de l'invention,
- la figure 2 représente le schéma de réalisation pratique des moyens de contrôle des clés électroniques selon l'invention,
- la figure 3 représente le schéma de réalisation pratique d'un support de mémorisation selon l'invention.

Dans toute la suite de la description on entend par entité signataire ou entité autorisée les moyens d'élaboration des clés électroniques, c'est dire des couples S, DH (signatures électroniques et données), ces moyens permettant en outre le chargement de ces signatures dans les supports de mémorisation. On entend par serrure électronique les moyens de contrôle des données lues dans les supports de mémorisation.

L'entité signataire est selon l'invention apte à produire une signature électronique S à partir d'une fonction de production f et d'une clé K secrète.

La signature électronique d'une donnée DH par l'entité signataire peut donc s'écrire S = f (K, DH).

Afin que la signature de l'entité signataire puisse être vérifiée par chacune des serrures électroniques susceptibles de fournir l'accès, ces serrures disposent de moyens cryptographiques adéquats. Ces moyens se décomposent en un algorithme de vérification f' et une clé de vérification K' qui selon que l'algorithme de signature est à clé secrète ou à clé publique est égale à la clé secrète ou publique de l'entité signataire. Dans le premier cas on a donc K = K', dans le second cas il sera impossible connaissant K' d'en déduire K.

Selon les applications prévues les serrures électroniques seront placées, soit dans un environnement public, soit dans un environnement privé. Dans les cas où les serrures électroniques sont placées dans un environnement public, on utilisera de préférence un algorithme à clé publique de sorte que ces serrures électroniques ne contiennent aucune information secrète et qu'il n'y ait pas d'intérêt à en lire frauduleusement le contenu. Ainsi, on augmente la sécurité du système et on décourage donc le vandalisme en le rendant sans objet.

Ainsi selon l'invention, le support de mémorisation a alors une fonction de clé électronique apte à ouvrir toutes les serrures électroniques implantées sur tout un territoire ou sur une zone particulière. Selon l'invention, la fonction clé électronique est obtenue à partir d'une donnée relative à une période prédéterminée d'autorisation d'accès limitant la validité du support. Cette période se trouve sous forme par exemple d'une date et heure de début de plage horaire et date et heure de fin de plage horaire que l'on note dans la suite DH. Il peut s'agir également d'une date et d'une heure de fin d'autorisation. Lors du contrôle d'accès, la serrure électronique qui est

avantageusement dotée d'une horloge interne vérifie que l'information date/heure courante se trouve bien à l'intérieur de la plage puis, vérifie la signature à l'aide de la clé de vérification (secrète ou publique selon le cas) dont elle dispose. Si les deux vérifications sont satisfaites la serrure envoie un signal d'autorisation d'accès A.

A titre d'exemple, dans le cas où un algorithme à clé secrète est utilisé, la serrure électronique lit la plage DH enregistrée dans le support de mémorisation, lit à partir de son de l'horloge interne l'information date et heure courante et vérifie que cette information se trouve dans la plage lue dans le support puis, calcule une signature $S' = f(K, DH)$. La serrure va lire également la signature qui a été mémorisée dans le support et vérifie que la signature calculée est égale ou non à la signature lue.

Dans le cas où l'on utilise un algorithme à clé publique, alors la serrure électronique lit la donnée relative à la plage horaire DH, lit la date et heure donnée par son horloge interne et vérifie que cette date et heure courantes se trouvent bien dans la plage lue dans le support de mémorisation. La serrure électronique va également lire la signature S mémorisée dans le support et vérifie à l'aide de la fonction de vérification f' et de la clé publique K' associée à K que cette signature S est bien la signature de la donnée DH ce qui peut s'exprimer sous la forme :

$f'(K', DH, S) = \text{"OK"}$,

l'information "OK" correspondra en pratique à 1 bit à 1 ou à 0 selon la convention adoptée.

La description qui va suivre va maintenant détailler des modes de réalisation pratiques. On pourra se reporter aux figures 1 à 3 pour mieux comprendre.

Comme cela a été précisé, le système selon l'invention permet d'éviter d'avoir à tenir des listes noires et d'avoir à gérer de telles listes à chaque demande d'accès à des bâtiments, ou à des systèmes informatiques, ou à toutes autres sortes d'objets comme cela doit être fait avec les techniques de l'art antérieur.

Ainsi pour atteindre ce but, l'invention substitue aux moyens d'accès mécaniques traditionnels associés à une clé mécanique un moyen logique résidant en une signature électronique calculée par une entité autorisée ayant reçu pour cela une clé K secrète.

L'invention consiste donc en outre à charger une signature électronique dans chaque support. La donnée signée par cette signature électronique comporte une donnée relative à une période prédéterminée de validité d'utilisation. Ainsi, en dehors de cette période de validité d'utilisation, la signature n'est plus reconnue et l'accès n'est donc pas autorisé. Si le chargement d'une nouvelle signature n'a pas eu lieu l'accès ne sera donc plus autorisé.

On a représenté sur la figure 1 le schéma d'un système selon l'invention. Ce système comporte des moyens d'élaboration des signatures électroniques LE. En pratique, ces moyens pourront être réalisés par un lecteur encodeur comportant un microprocesseur ou un microcontrôleur, programmé de manière à mettre en oeuvre un algorithme de production f. Il pourra s'agir par exemple d'un algorithme à clé secrète ou d'un algorithme à clé publique connu.

On peut citer à titre d'exemple comme algorithme à clé secrète l'algorithme DES (Data Encrytion Standard) et comme algorithme à clé publique l'algorithme RSA (Rivest Shamir Adleman).

Dans la suite de la description, ces algorithmes vont être représentés par une fonction f.

Le lecteur/encodeur permet en outre de charger les signatures dans les supports de mémorisation. Pour cela, on choisit un lecteur/encodeur connu et adapté au support de mémorisation choisi. On pourra prendre à titre d'exemple des lecteurs/encodeurs existants sur le marché permettant de lire et d'écrire dans une carte magnétique ou dans une carte à mémoire à contact affleurant ou un lecteur/encodeur adapté à la lecture et à l'écriture sur une clé électronique à contact affleurant ou un lecteur/encodeur adapté à la lecture et à l'écriture de cartes sans contact.

L'exemple illustré sur la figure 1 montre le schéma électronique d'un lecteur/encodeur adapté à la lecture et à l'écriture sur un support de mémorisation de type carte à mémoire.

Ce lecteur/encodeur est de type connu et comporte un microprocesseur 100 (ou microcontrôleur) avec une mémoire de programme associée 101 de type ROM ou EEPROM (électriquement effaçable) et éventuellement une mémoire de travail 103 de type RAM.

Ce lecteur/encodeur LE comporte une interface d'entrée/sortie 103 adaptée au support de mémorisation. Il comportera soit une antenne d'émission/réception dans le cas de support à lecture/écriture sans contact. Il comportera des contacts adaptés aux contacts affleurants tels que ceux des cartes à puces ou des clés électroniques. Ce lecteur comporte en outre un clavier non représenté.

La mémoire non volatile 101 du lecteur/encodeur LE contient le programme de mise en oeuvre de la fonction f choisie et un programme classique de lecture et

écriture sur un support de mémorisation. La clé K sera également enregistrée dans cette mémoire.

La signature calculée peut être la même pour tous les supports. Si la signature S est la signature d'une donnée DH, alors cela signifiera que cette donnée DH est la même pour tous les supports.

Les signatures calculées peuvent être différentes pour chaque support.

Les signatures S destinées à chaque support peuvent alors être calculées par avance ou au coup par coup. Dans le cas où elles sont calculées d'avance, il faut que les données DH relatives à chaque utilisation soient enregistrées dans une mémoire non volatile du lecteur/encodeur. Dans ce cas on mémorisera également une table afin de faire correspondre à chaque utilisation le couple : signature S - donnée DH qui lui est affectée.

Dans ce cas, lorsqu'un support de mémorisation est introduit dans le lecteur/encodeur par un utilisateur, l'utilisateur peut saisir son numéro d'identification sur le clavier du lecteur/encodeur et le lecteur/encodeur va aller chercher dans la table la signature S et la donnée DH qui est affectée à cette utilisation et les charger dans la mémoire du support.

Bien entendu, on pourra procéder de façon différente sans que cela change le principe de l'invention. En effet, le système dans lequel les signatures peuvent être calculées au fur et à mesure du besoin, c'est à dire à chaque demande de chargement dans le support de mémorisation faite par un utilisateur. Dans ce cas, il n'est pas nécessaire de mémoriser une table contenant les différentes signatures et les différentes données relatives à chacun des utilisateurs. L'utilisateur entre lui-même

la donnée DH qui lui est propre et le calcul est fait en temps réel par le lecteur/encodeur LE.

Les signatures produites peuvent être différentes parce que les clés de production choisies sont différentes. Cette différence peut être introduite par une donnée Z prédéterminée permettant de distinguer des zones d'utilisation soit géographiques, soit logiques. Il s'agira de zone logique dans le cas où il s'agirait d'autoriser des accès à certains programmes et pas d'autres dans un système informatique.

Selon l'invention, les bâtiments ou les systèmes soumis à un contrôle d'accès sont en outre équipés d'un moyen de vérification du type serrure électronique qui, dans l'application particulière qui est décrite, sera constitué d'un lecteur de type lecteur de cartes soit à contacts affleurants tels que représenté sur la figure 2, soit un lecteur à lecture sans contact, soit à lecture de pistes magnétiques, selon le support utilisé.

Ce lecteur L comporte de façon classique une unité de traitement 200 réalisée par un microprocesseur et des mémoires qui lui sont associées, une mémoire non volatile 201 et une mémoire de travail 202. Le lecteur comporte en outre une horloge interne 203. Dans la mémoire non volatile (par exemple du type ROM) se trouve programmée la fonction f de vérification de signature utilisée ainsi que la clé K utilisée pour vérifier les signatures.

Le support de mémorisation, quant à lui, comporte une mémoire non volatile 301 que l'on choisira de préférence reprogrammable électriquement (RAM sauvegardée ou EEPROM). Selon certaines applications, le support de mémorisation pourra comporter en outre une unité de traitement de type microprocesseur 300

avec une mémoire 302 associée de type ROM comportant une ou plusieurs fonctions de cryptage. Un tel support de mémorisation est schématisé sur la figure 3.

L'invention pourra être appliquée avantageusement à l'accès à des immeubles (et éventuellement aux boîtes à lettres) par les préposés au courrier.

Chaque préposé se verra alors attribué une clé électronique lui permettant d'accéder à tous les immeubles (et éventuellement aux boîtes à lettres de ces immeubles) d'une zone donnée, à l'intérieur d'une plage horaire donnée. Pour cela, on inscrira quotidiennement dans la clé un certain nombre d'informations caractéristiques de cette zone et de cette plage.

Bien entendu, l'invention peut être utilisée par toute autre organisation qui a besoin d'un accès fréquent à des immeubles. Dans cette application, toutes les données contenues dans les serrures électroniques affiliées à une zone donnée et relatives à une organisation donnée sont identiques, et la clé électronique détenue par un membre de cette organisation fait office de passe-partout électronique.

Une autre application possible est l'accès à une chambre d'hôtel. Le client d'un hôtel se voit attribué à son arrivée une clé électronique dont la mémoire contient des informations qui lui permettront d'ouvrir sa chambre (et, bien entendu, seulement celle-là) pour la durée exacte de son séjour. Le client n'a donc aucun intérêt à la dupliquer puisqu'elle cessera de fournir l'accès aussitôt qu'il aura quitté sa chambre. Dans cette application, les serrures électroniques ne contiennent pas toutes des données identiques et une clé électronique ne donne accès qu'à un seul ensemble protégé.

REVENDICATIONS

1. Système de contrôle d'accès au moyen d'un support de mémorisation portable (C), caractérisé en ce qu'il comporte :

1°) des moyens (LE) aptes à délivrer des clés électroniques formées au moins de données DH et de la signature S d'au moins ces données, ces moyens étant aptes à élaborer les signatures électroniques S des données DH relatives à une période d'autorisation d'accès prédéterminée et de charger les données DH et les signatures S dans les supports de mémorisation respectifs, une signature devant être recalculée pour établir le renouvellement des périodes d'autorisation d'accès.

2°) des moyens (L) assurant une fonction de serrure électronique aptes à délivrer un signal d'autorisation d'accès A dans le cas où le support de mémorisation (C) comporte en mémoire la donnée et la signature requise, ces moyens étant aptes à vérifier que la donnée est bien la donnée attendue et que la signature est la signature de cette donnée.

2. Système de contrôle d'accès selon la revendication 1, caractérisé en ce que la donnée DH relative à une période prédéterminée de validité comporte une information de date d'utilisation et une plage horaire d'utilisation.

3. Système de contrôle d'accès selon la revendication 1 ou 2, caractérisé en ce que les moyens

(L), assurant la fonction de serrure, comporte une horloge interne (203) permettant de comparer la donnée mémorisée DH à la donnée temporelle temps réel H donnée par l'horloge; et des moyens pour vérifier que la signature S est bien la signature de la donnée DH, afin de délivrer ou non un signal d'autorisation d'accès selon le résultat de vérification obtenu.

4. Système de contrôle d'accès selon l'une quelconque des revendications 1 à 3, caractérisé en ce que les moyens d'élaboration des signatures (LE) comportent une unité de traitement (100) reliée à au moins une mémoire non volatile (101) dans laquelle sont enregistrées les données DH et un algorithme f de signature des données de sorte que S = f (K, DH), K étant une clé secrète et l'algorithme f est un algorithme à clé secrète ou à clé publique.

5. Système de contrôle d'accès selon l'une quelconque des revendications précédentes, caractérisé en ce que la clé K utilisée pour élaborer les signatures est la même pour toutes les signatures chargées dans les supports et renouvelées.

6. Système de contrôle d'accès selon l'une quelconque des revendications précédentes, caractérisé en ce que pour distinguer différentes zones géographiques ou logiques d'utilisation, on associe à la clé K une donnée Z distincte selon les zones.

7. Système de contrôle d'accès selon l'une quelconque des revendications 1 à 4, caractérisé en ce que l'on utilise des clés différentes pour élaborer les

signatures, une clé étant choisie par zone géographique ou logique prédéterminée.

8. Système de contrôle d'accès selon l'une quelconque des revendications précédentes, caractérisé en ce que la clé utilisée est une clé diversifiée K_C = Div (K,C), C étant une donnée prédéterminée et Div une fonction de diversification.

9. Système de contrôle d'accès selon l'une quelconque des revendications précédentes, caractérisé en ce que la plage horaire de validité déterminée est formée de plusieurs plages horaires consécutives et en ce que les moyens délivrant les clés électroniques élaborent une signature Si pour chacune de ces plages.

10. Système de contrôle d'accès selon l'une quelconque des revendications précédentes, caractérisé en ce que les moyens assurant la fonction de serrure électronique (L) comportent une unité de traitement (200) et au moins une mémoire non volatile (201) dans laquelle sont enregistrés l'algorithme de vérification de signature et la clé de vérification de signature..

11. Système de contrôle d'accès selon la revendication 10, caractérisé en ce que les moyens assurant la fonction de serrure électronique (L) sont adaptés à la lecture des supports de moyens de mémorisation (C).

12. Système de contrôle d'accès selon la revendication 11, caractérisé en ce que les moyens assurant la fonction de serrure électronique sont

formés d'un lecteur de carte à mémoire ou de clé électronique.

13. Système de contrôle d'accès selon la revendication 12, caractérisé en ce que le lecteur est un lecteur de cartes magnétiques, ou de carte à puce à contact affleurant, ou un lecteur U de cartes à puce sans contact.

14. Système de contrôle d'accès selon l'une quelconque des revendications précédentes, caractérisé en ce que les supports de mémorisation (C) comportent une mémoire non volatile reprogrammable électriquement (RAM sauvegardée, EEPROM).

15. Système de contrôle d'accès selon la revendication 14, caractérisé en ce que les supports (C) sont réalisés, soit par des cartes à mémoire à contact affleurant, soit par des cartes à mémoire à lecture sans contact, soit par des clés électroniques soit par des cartes magnétiques.

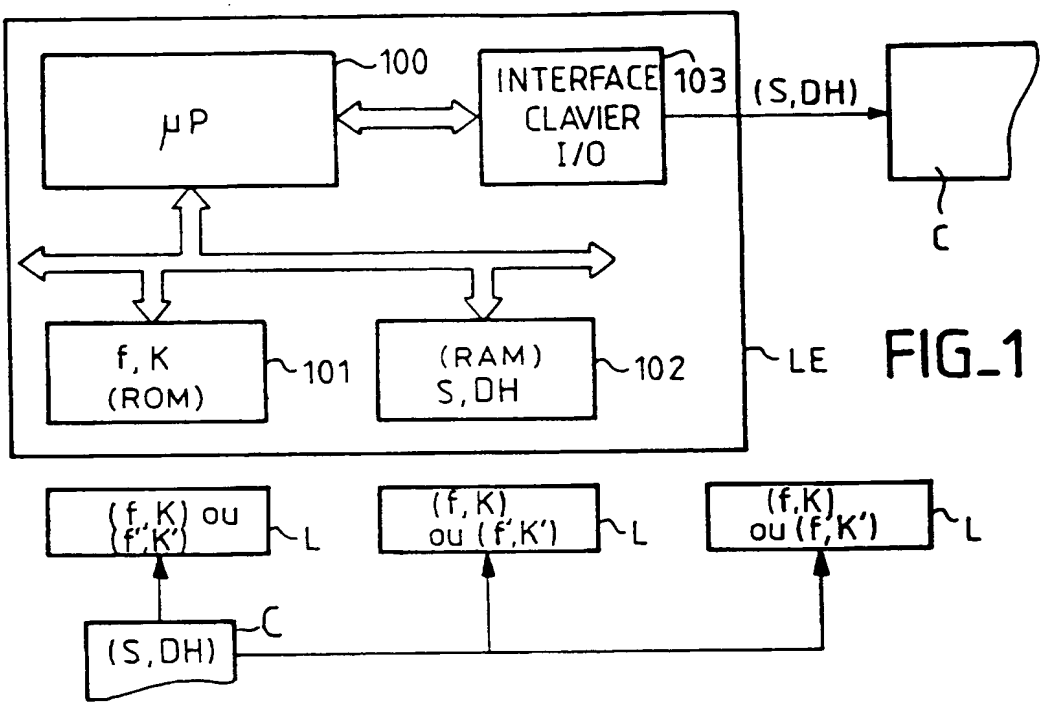


FIG_1

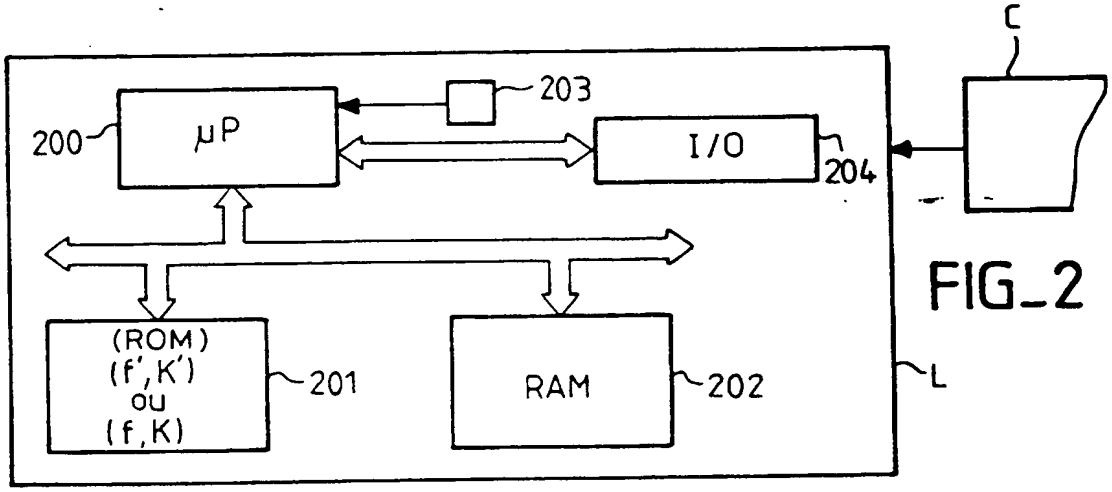


FIG_2

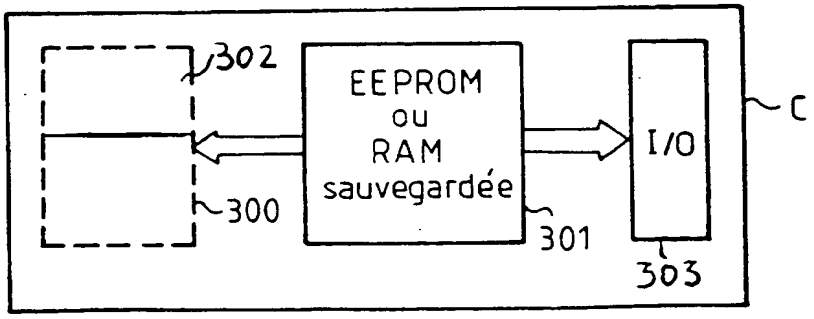


FIG_3

REPUBLIQUE FRANÇAISE

2722596

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 502819
FR 9408770

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée	
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	EP-A-0 299 826 (SCHLUMBERGER INDUSTRIES) * colonne 5, ligne 22 - colonne 8, ligne 14; figures * ---	1,4,5, 11-15	
A	EP-A-0 122 244 (WSO CPU-SYSTEM) * abrégé; revendications; figures * ---	1-3,6, 10-13,15	
A	EP-A-0 030 381 (THE GREY LAB. ESTABLISHMENT) * abrégé; revendications; figures * * page 9, ligne 4 - page 10, ligne 5 * ---	1	
A	WO-A-91 18169 (MEDECO SECURITY LOCKS) * page 5, ligne 29 - page 8, ligne 29 * * page 10, ligne 20 - page 12, ligne 29; figures * ---	1-4	
A	US-A-4 720 860 (WEISS) * colonne 1, ligne 39 - colonne 3, ligne 45 * * colonne 6, ligne 5 - ligne 49; revendications; figures * ---	1-3,5	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6) G07C G07F
A	US-A-4 453 074 (WEINSTEIN) * abrégé; figures * ---	1	
A	EP-A-0 422 757 (FISCHER) * abrégé; revendications; figures * * colonne 2, ligne 32 - colonne 3, ligne 23 * * colonne 3, ligne 58 - colonne 8, ligne 5 * ---	1	
A	EP-A-0 253 722 (BULLCP8) -----		

1

Date d'achèvement de la recherche	Examinateur
13 Avril 1995	Meyl, D

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

THIS PAGE BLANK (USPTO)